Risk Committee Charter

SUNCORP

ISSUE DATE: 12 DECEMBER 2024

Introduction

This is the Charter of the Board Risk Committee. The Board Risk Committee, appointed by the Board of the Company specified in item 1 of the Schedule also operates as the Board Risk Committee for the Group, and performs the functions outlined in this Charter, for each of the entities (if any) specified in item 2 of the Schedule except where the entity specified in item 2 of the Schedule has appointed its own risk committee.

The purpose of the Board Risk Committee is to provide oversight across the Group for all categories of risk, and risk culture. In this role, the Board Risk Committee has the delegated authority from the Board to approve and oversee the processes used to identify, evaluate and manage risk. At its discretion, the Board Risk Committee may make recommendations to the Board, including recommendation of the Group's risk appetite.

Definitions

The following terms have the following meanings:

"**Board**" means the board of the Company and the board of each of the entities specified in item 2 of the Schedule, except for those entities which have appointed their own risk committee or adopted their own risk committee charter.

"**Board Risk Committee**" means the Board risk committee of the Group.

"**Company**" means the company specified in item 1 of the Schedule.

"**Company Secretary**" means the company secretary of the Company and of the entities (if any) specified in item 2 of Part A of the Schedule.

"**Group**" means the company specified in item 1 of the Schedule and the entities (if any) specified in item 2 of the Schedule.

"**Senior Executive**" means a senior executive position directly reporting to the CEO & Managing Director.

"**Specified Roles**" means a person who is a senior manager, executive director, material risk-taker (including highly-paid material risk-takers) and risk and financial control personnel, as outlined in APRA's Remuneration Prudential Standard CPS 511.

"**Suncorp Group**" means the Suncorp Group Limited group of companies.

Role

The Board Risk Committee is responsible for performing the duties set out in this Charter to enable the Board to fulfil its oversight responsibilities in relation to the Group's:

- risk and compliance management, frameworks and strategies, ensuring that they remain appropriate to the size, business mix and complexity of the Group, and are consistent with the Group's business plan;
- risk culture assessment, monitoring, and activities to drive improvements;
- identification, assessment, management, and improvement of risk and compliance effectiveness.

The scope of the Board Risk Committee is all categories of risks as defined in the Enterprise Risk Management Framework, being Strategic, Financial, Insurance, Operational, and Emerging.

Composition

The Board Risk Committee will be appointed by the Board and shall comprise not less than three directors. All members of the Board Risk Committee must be non-executive directors, and a majority of members must be independent.

Chairman

The Board shall appoint one of the Board Risk Committee members to serve as the Board Risk Committee Chairman. The Board Risk Committee Chairman shall be an independent director. The Board Risk Committee Chairman will not be the Chairman of the Board. The Board Risk Committee Chairman and membership will be confirmed annually.

Administrative Matters and Procedures

Meetings shall be held at a frequency determined by the Board Risk Committee but in any event not less than four times per year. Special meetings may be convened by the Board Risk Committee Chairman as required.

A quorum of any meeting will be two members or such other number determined by the Board. The agenda and supporting documentation will be circulated to the Board Risk Committee members in a reasonable period in advance of each meeting.

Board members, who are not Board Risk Committee members, will receive copies of the agenda and supporting documentation for each meeting of the Board Risk Committee and may attend meetings of the Board Risk Committee as observers.

Non-Board Risk Committee members may attend part or all of any meeting of the Board Risk Committee at the invitation of the Board Risk Committee Chairman. The Board Risk Committee Chairman will offer standing invitations to the CEO & Managing Director, the Chief Risk Officer, the External Auditor and the Executive General Manager Internal Audit. Specific invitations will be offered to other Senior Executives to lead discussions in their areas of accountability where required.

The secretary of the Board Risk Committee will be the Company Secretary, or such other person as nominated by the Board. The secretary of the Board Risk Committee will circulate minutes to members of the Board Risk Committee and the Board as soon as practicable after each meeting.

Any time sensitive matters that may require engagement of the Board Risk Committee in between meetings should be raised by the CEO & Managing Director or the Chief Risk Officer with the Board Risk Committee Chairman. The Board Risk Committee Chairman will determine if a formal Board or Board Risk Committee meeting needs to be convened or how the Board Risk Committee members will be otherwise informed. In addition, any Board Risk Committee members may raise a time sensitive matter directly with the Board Risk Committee Chairman outside of the scheduled meetings.

Further, the Board Chairman may determine, in consultation with the Board Risk Committee Chairman, that a particular matter set out in the Duties and Responsibilities section of this Charter should receive consideration at a Board meeting.

Reporting

The Board Risk Committee shall submit an update to the Board, summarising the Board Risk Committee activities and outlining any approvals or recommendations, after each Board Risk Committee meeting.

The Board Risk Committee shall submit an annual Letter of Representation to the Board Audit Committee confirming the status of material risk issues considered by the Board Risk Committee that are open at the end of the financial year and a summary of key risks considered by the Board Risk Committee.

The Board Risk Committee shall review and provide input into an annual paper, prepared by the Chief Risk Officer and submitted to the Board People and Remuneration Committee, regarding significant matters that are relevant to remuneration consequences for persons in Specified Roles.

Duties and Responsibilities

The Board Risk Committee shall:

- recommend for Board approval and oversee the Group's **Risk Management and Compliance Strategies** and the **Enterprise Risk Management Framework (ERMF)**;
- review and recommend to the Board the **Risk Appetite Statements** for the Group and its Australian general insurance entities and oversee adherence to the approved Risk Appetite Statements;
- review, monitor and challenge the Group's **risk profile, adequacy of risk management activities and management actions**, including:
  - performance against the Risk Management Strategies, and the operation of the ERMF;
  - management's assessment of key current and emerging risk and compliance exposures. These may include consideration of external developments, regulatory change, organisational change, customer risks, major initiatives, transition services arrangements, product development and material outsourcing activities;
  - oversight of the Group's control environment to ensure controls are accurately rated, adequately designed and appropriately described;
  - reports and deep dives from senior management across the business, that highlight key risks and issues and management actions;
  - actions being taken to manage risks within risk appetite, including challenging where there is opportunity to take more considered risk;
  - actions being taken to monitor and strengthen risk and compliance management practices;
  - actions to address significant risk incidents and compliance breaches, including "lessons learned", customer remediation and thematic or systemic trends that drive customer risk including vulnerability and hardship;
  - monitor risk assessment activities relating to **customer, conduct and reputational risks** to ensure consideration of fair customer outcomes and meeting of community standards;
- oversee the Group's **information security posture**, including management actions to evaluate threats and improve the cyber security control environment;
- oversee the Group's legal, regulatory, industry code and policy **compliance processes** including breach management, regulatory engagement, and management actions to ensure compliance practices are adequate;

- oversee management's assessment of **risk culture**, the extent to which that culture supports the ability of the Group to operate consistently within its risk appetite, and actions to ensure a sound risk culture is maintained;

- review and approve or recommend for Board approval any new, material variation in, or repeal of **Group Policies** that are material to the operation of the ERMF;

- review and approve the **Intra-Group Transactions and Exposure Limits** and **Aggregate Risk Exposures** and consider reports from management that monitor the exposures against the approved limits;

- review and consider the approach to extreme and rare risks, including the Group's **capital stress testing** where relevant to setting the Group's risk appetite and evaluating aspects of the Group's risk management;

- review and recommend to the Board the Group's **Internal Capital Adequacy Assessment Process** (ICAAP) – comprising the ICAAP Report, ICAAP Summary Statement, and Capital Recovery and Exit Plan – and ensure that the Group maintains a sound capital base to support the risks undertaken, aligning with the Group's strategic objectives and regulatory requirements;

- review and recommend to the Board the **Reinsurance Management Strategy** and provide oversight of the **Reinsurance Arrangements Statement**. Ensure that reinsurance strategy and arrangements align with Suncorp's risk management framework and regulatory requirements;

- review and consider reports from **internal and external audit** that are relevant to the Committee's role;

- review and recommend to the Board **annual regulatory statements** relating to governance and risk management, including the APRA Risk Management Declaration;

- review and endorse the significant matters that should be considered by the Board People and Remuneration Committee for remuneration consequences for persons in Specified Roles;

- review and consider an **independent report on the appropriateness, effectiveness and adequacy of the ERMF**, against prudential requirements as required, or at least every three years;

- request any further information from management to be appropriately informed of matters in executing its responsibilities including engagement and consultation with independent experts to carry out its responsibilities. In doing so, the Board Risk Committee may rely on the advice of experts.

Other Responsibilities

The Board Risk Committee shall:

- provide prior endorsement for the appointment of and removal of the Chief Risk Officer on the recommendation of the CEO & Managing Director;

- monitor the performance and objective setting of the Chief Risk Officer in consultation with the CEO & Managing Director;

- regularly review this Charter and its adequacy. The Board Risk Committee shall, as required, recommend changes to the Charter to the Board for approval;

- be available to meet regulators on request.

Interaction with the Board and Other Committees

The Chairman of the Board Risk Committee will periodically meet with the Chairman of the:

- Board;
- Board Audit Committee;
- Board People & Remuneration Committee;
- Other standing committees of the Board as appropriate,

to consider and share key information identified by those committees.

Matters requiring the attention of the Board and other committees will be circulated to the appropriate committee by the secretary of the Board Risk Committee.

Function of Representative Parties

Members of the Board Risk Committee are not full-time employees of the Group. As such, it is not the responsibility of the Board Risk Committee personally to conduct risk management reviews.

The Senior Executives are responsible for identifying, assessing and managing risk within the Group's risk appetite and framework, and implementing systems to effectively manage compliance obligations. Senior Executives will provide regular updates to the Board Risk Committee on these activities, where appropriate, and will escalate issues to the Board Risk Committee for its review as and when appropriate.

The Chief Risk Officer is responsible for defining the risk management process and frameworks, providing challenge to the first line of defence on risk management activities, assessing risks and reporting to the Board Risk Committee. The Chief Risk Officer may rely upon information contained within risk systems and reports prepared by management in accordance with the three lines of defence model.

Internal Audit is responsible for independent assurance over the effectiveness of the systems of controls and the application of the ERMF.

Rights of Access and Authority

Each member of the Board Risk Committee has rights of access to executives, risk and financial control employees, Appointed Actuaries, Internal Audit and External Audit without any other management present, and rights to seek explanations and additional information from both management and auditors, in order to fulfil their role and undertake their duties.

The Board Risk Committee Chairman will provide the Chief Risk Officer and the Risk Function with clear rights of access to the Board Risk Committee and the Board.

Schedule: Risk Committee Charter

Item 1: Name of Company

Suncorp Group Limited

Item 2: Name of Entities

Suncorp Insurance Holdings Limited, Suncorp Life Holdings Limited and all other APRA-regulated entities within the Suncorp Group of Companies.